United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES,
Plaintiff,
v.
GEORGE VORTMAN,
Defendant.

Case No. 16-cr-00210-TEH-1

ORDER DENYING DEFENDANT'S MOTION TO DISMISS FOR OUTRAGEOUS GOVERNMENT CONDUCT AND MOTION TO SUPPRESS NIT SEARCH WARRANT

On August 19, 2016, Defendant Vortman filed a Motion to Dismiss Indictment for Outrageous Government Misconduct (ECF No. 54) and a Motion to Suppress NIT Search Warrant (ECF No. 55). The Government timely opposed both motions, and Vortman timely replied to each opposition. The Court heard oral arguments on both motions on December 5, 2016. After carefully considering the parties' written and oral arguments, the Court DENIES both of Vortman's motions for the reasons set forth below. The Court shall first address Vortman's motion to dismiss, and then address his motion to suppress.

I. BACKGROUND

Playpen was a website dedicated to sharing and distributing child pornography that operated as a "hidden service" on The Onion Router ("Tor"). ECF No. 58-1, at 5–39 ("Macfarlane Aff.") ¶ 6. Tor protects a user's identity by concealing the user's internet protocol address ("IP address").[1] Instead of directly connecting to a website using the user's IP address, the Tor software conceals the user's true IP address by bouncing the user's communications through an intermediary network of relay computers ("nodes"). *Id.* ¶ 8. As a result, when the Tor user finally connects to a website, the IP address visible to

[1] "[An] IP address is a unique identifier assigned by an internet service provider ("ISP") to a subscriber that can be used to determine the physical location of the subscriber if cross-referenced with the ISP's records." *United States v. Conner*, 521 F. App'x 493, 495 (6th Cir. 2013).

that site is of the last relay computer through which the user's communications were routed ("exit node") – not the user's actual IP address. *Id.* In order to access the Tor network, users must install Tor software on their computer, which is freely available online. *Id.* ¶ 7. Because Tor conceals a user's IP address, normal law enforcement tools for identifying internet users are greatly frustrated. *See id.* ¶¶ 8, 29–30.

Tor also makes it possible for websites to be set up as "hidden services." *Id.* ¶ 9. Hidden services largely operate the same as regular public websites; however, there are several key differences. First, users can only reach these hidden services if the user is using the Tor client and operating in the Tor network. *Id.* Second, a hidden service's IP address[2] is hidden and replaced with a series of algorithm-generated characters, such as "asdlk8fs9dlflku7f" followed by the suffix ".onion." *Id.* Third, unlike regular websites on the "open" internet, the IP address of a computer hosting a hidden service cannot be looked up. *Id*. Fourth, Tor hidden services are not indexed like websites on the open internet. This means Tor users are unable to find hidden services using a traditional search browser. *Id.* ¶ 10. Therefore, users must know the exact web address of the website in order to access the site. *Id*. Tor users obtain the exact addresses of hidden services via direct communication with other users or from internet postings, which often contain a description of the websites contents. *Id*. In sum, due to the nature of hidden services, accessing them requires "numerous affirmative steps by the user, making it extremely unlikely that any user could simply stumble upon a website without understanding its purpose and content." *Id.*

The government began investigating Playpen in September 2014. *Id.* ¶ 11. Upon arriving at the site a user would see two images of partially clothed prepubescent females with their legs spread apart, along with text stating, "No cross-board reports, .7z preferred, encrypt filenames, include preview, Peace out." *Id.* ¶ 12. This text referred to a ban against reposting material from other websites and the preferred method of compressing

[2] Like computers browsing the internet, websites also have unique IP addresses. *United States v. Forrester*, 512 F.3d 500, 510 n. 5 (9th Cir. 2007).

large files for distribution. *Id*. The main page also contained data-entry fields for login credentials and a separate link for users who wanted to register an account with Playpen. *Id*. Upon clicking this separate link, users would see a message informing them that new account registration required an email address but also instructing users to enter "something that matches the xxx@yyy.zzz pattern" rather than a real address. *Id.* ¶ 13. The same message encouraged users to take additional measures when using Playpen to protect their identity, such as turning off Javascript. *Id*. Upon logging into the website, users would see an extensive list of sections, forums, and sub-forums. The forums were organized into various sections based on content such as "Jailbait Videos," "Jailbait Photos," "Pre-teen Videos," "Pre-teen Photos," "Webcams," "Potpourri," and "Kinky Fetish." *Id.* ¶ 14. Several sections were further sub-categorized by gender and the type of child pornography contained (e.g., hardcore, softcore, and non-nude). *Id*. Typical posts within these forums contained text, images, compressed files, and links to external sites. *Id.* ¶ 16. The site also permitted private messages to be sent between Playpen users, *Id.* ¶ 20; the uploading of images and videos of child pornography, which would then be available to all Playpen users, *Id.* ¶¶ 23–24; and chat rooms where logged-in Playpen users could communicate with each other and share images, *Id.* ¶ 25.

In December 2014, based on a tip from a foreign law enforcement agency, the FBI linked Playpen's IP address to a server in North Carolina. *Id.* ¶ 28. In January 2015, the government executed a search warrant, seized the suspected server, and confirmed the server contained a copy of the Playpen website. *Id*. Because Playpen's IP address log contained only the "exit nodes" of its users[3], the government was unable to locate and identify Playpen users. *Id.* ¶ 29. Although the government considered immediately shutting down the website permanently, the government also recognized this action would have prevented the government from identifying the users who possessed, distributed, and

[3] While the government offers no explanation – perhaps because part of the footnote is redacted – it appears Playpen's server contained the true IP address of an amount "less than 1% of [its] registered users." *Id.* ¶ 29 n. 7.

received child pornography, and also from potentially rescuing child victims from ongoing abuse. ECF No. 54-4, at 7. Instead, the government sought a warrant allowing it to run Playpen from its server for thirty days and to deploy a network investigative technique ("NIT") against individuals who logged into Playpen using both a username and password. *See generally* ECF No. 58-1. The warrant application explained that during the normal course of operation, websites send content to visitors, which a user's computer downloads and uses to display the webpages. Macfarlane Aff. ¶ 33. In accordance with the NIT warrant, the government planned to "augment" Playpen's website with additional computer instructions – the NIT – that would cause the user's computer to transmit identifying information to a government computer. *Id.*

On February 20, 2015, the NIT warrant was approved for a thirty-day period and signed by Theresa Buchanan, a Magistrate Judge of the Eastern District of Virginia. *See* ECF No. 58-1, at 1. The warrant described the place to be searched as:

> This warrant authorizes the use of a network investigative technique ("NIT") to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below.
>
> The computer server is the server operating the Tor network child pornography website [Playpen], as identified by its URL –upf45jv3bziuctml.onion – which will be located at a government facility in the Eastern district of Virginia.
>
> The activating computers are those of any user or administrator who logs onto [Playpen] by entering a username and password. The government will not employ this network investigative technique after 30 days after this warrant is authorized, without further authorization.

Id. at 3. Attachment B described the "Information to be Seized" from any "activating computer": (1) the IP address of the computer and the date and time this information is determined; (2) a unique identifier that distinguishes the data from other "activating" computers; (3) the type of operating system running on the computer; (4) information on whether the NIT had already been delivered to the computer; (5) the computer's host name; (6) the computer's active operating system username; and (7) the computer's media access control ("MAC") address. *Id.* at 4.

During the duration of the warrant "the FBI did not post any images, videos, or links to images or videos of child pornography." ECF No. 54-4, at 5. Images, videos, and links that were posted before the FBI obtained control of the website remained available to site users. *Id.* at 5–6. However, "FBI Special Agents monitored all site postings, chat messages, and private messages twenty-four hours per day" in order to assess and mitigate any risk of imminent harm to children. *Id.* at 6. The government also held regular meetings to discuss the status of Playpen based on several factors including site users' continued access to child pornography, the risk of imminent harm to a child, the need to identify and apprehend perpetrators of those harms to children, and other factors. *Id.* at 8. On March 4, 2015, the government decided the balance of these factors weighed in favor of shutting down the website. *Id.*

Using information provided by the NIT, the FBI found someone had registered an account with Playpen on January 3, 2015 under the username "childpornstar." ECF No. 58-2, ¶¶ 27–28. Further investigation revealed that "childpornstar" had accessed an online posting titled "Deep Anal (updated Mirrors)" within a section titled "Pre-teen Videos >> Girls HC [Hardcore]." *Id.* ¶ 30. The same user also accessed online posts in the "Girls HC [Hardcore]" forum containing links to compilations of images depicting images of child pornography. These compilations included several images of pre-pubescent girls being sexually abused and exploited. *Id.* ¶¶ 33–34. Playpen's logs demonstrated "childpornstar" had actively logged onto the website for a total of eighteen hours and thirteen minutes between January 3, 2015 and March 4, 2015. *Id.* ¶ 28. Using the IP address revealed for "childpornstar" by the NIT, the FBI traced the IP address to a residence in San Francisco. *Id.* ¶ 36. The FBI later identified Vortman as the identity behind "childpornstar" and, in August 2015, applied for a search warrant to search Vortman's residence. *Id.* ¶¶ 37–42, 55. The search warrant was signed by Magistrate Judge Joseph Spero on August 25, 2015. *See id.* at 1. A search of Vortman's residence discovered over 1,000 images and over 150 videos of child pornography on Vortman's desktop computer, some of which depicted the rape of prepubescent minors, sadistic and masochistic abuse, and bestiality. ECF No. 58-3.

On May 17, 2016, Vortman was indicted on one count of receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B), (b)(2). ECF No. 40.

II. MOTION TO DISMISS INDICTMENT FOR OUTRAGEOUS GOVERNMENT MISCONDUCT

A. Legal Standard

Outrageous government conduct occurs when the actions of law enforcement officers are "so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction." *United States v. Russell*, 411 U.S. 423, 431–32 (1973). In order for a defendant to succeed on a motion to dismiss for outrageous government conduct, the defendant must meet the "extremely high standard" of demonstrating the facts underlying his arrest and prosecution are so "extreme" as to "violate fundamental fairness," or are "so grossly shocking . . . as to violate the universal sense of justice." *United States v. Black*, 733 F.3d 294, 298 (9th Cir. 2013). In making this determination, the Ninth Circuit has established six factors courts must consider:

> (1) known criminal characteristics of the defendants; (2) individualized suspicion of the defendants; (3) the government's role in creating the crime of conviction; (4) the government's encouragement of the defendants to commit the offense conduct; (5) the nature of the government's participation in the offense conduct; and (6) the nature of the crime being pursued and necessity for the actions taken in light of the nature of the criminal enterprise at issue.

Id. at 303. While none of these factors are dispositive, nor do they create "a formalistic checklist," they focus the court's analysis on the totality of the circumstances. *Id.* at 304. And because "[t]here is no bright line dictating when law enforcement conduct crosses the line between acceptable and outrageous, [ ] 'every case must be resolved on its own particular facts.'" *Id.* at 302 (quoting *United States v. Bogart*, 783 F.2d 1428, 1438 (9th Cir. 1986)).

B. Discussion

a. Vortman's Motion to Dismiss is Foreclosed by *United States v. Mitchell*

As an initial matter, Vortman's motion for dismissal is barred by *United States v. Mitchell*, 915 F.2d 521 (9th Cir. 1990). In that case, the government had created a sting operation to capture individuals knowingly receiving child pornography. *Id.* at 521. The government sent an unsolicited four-page application for membership to "Loveland", a fictitious entity created by the government, which advocated "the right to seek pleasure without the restrictions being placed upon us by an outdated puritan morality." *Id.* at 523. Applicants were required to complete a survey to express their attitude towards sexual activities, including "sexually explicit materials, sexual freedom in all activities, and sexual freedom for all consenting persons without any age restrictions." *Id.* The government would send a follow-up mailing from another fictitious organization, the Far Eastern Trading Company, offering to sell child pornography to individuals who submitted completed surveys indicating pedophilic tendencies. *Id.* at 524–25. Individuals who ordered the material would be arrested upon receiving the child pornography. *Id.* at 523–24. The defendant in *Mitchell* completed the Loveland survey, received a catalog from the Far Eastern Trading Company, placed an order for a child pornography magazine, and was arrested once he picked up the magazine from the post office. *Id.* at 523–24. The defendant moved to dismiss his indictment arguing the government's conduct was outrageous, which the district court denied. *Id.* at 522. The Ninth Circuit affirmed the district court, finding that while the government's conduct was "particularly offensive," it did not violate notions of fundamental fairness. *Id.*at 526 and n.8. In particular, the court highlighted the fact that even though the government "orchestrated the operation," the defendant was not threatened or coerced into purchasing child pornography. Rather the defendant responded to the solicitation voluntarily. *Id.* at 526.

Here, like the defendant in *Mitchell*, Vortman's actions in using Playpen to access child pornography were completely voluntary. The government did not threaten, coerce, or prod him to use Playpen. In fact, Vortman had already created an account with Playpen

and was using the site before the government started its sting operation. *See* ECF No. 58-2, at 11. Also, unlike the sting operation in *Mitchell* where the government "orchestrated" the child pornography enterprise and distributed child pornography, here the government merely attached itself to a child pornography operation that was already in full operation. Because the government's conduct here is less offensive than the sting operation in *Mitchell*, dismissal of Vortman's indictment is unwarranted.[4]

b. All Six *Black* Factors Weigh Against Dismissing Vortman's Indictment

Additionally, consideration of the six *Black* factors also requires a finding that the government's conduct here was not outrageous. The first two *Black* factors weigh against dismissal. The first factor, "known criminal characteristics of defendants," looks at "whether a defendant had a criminal background or propensity the government knew about when it initiated its sting operation." *Black*, 733 F.3d at 304. The second factor, "individualized suspicion of the defendants," considers "[w]hether the government had reason to suspect an individual or identifiable group before initiating a sting operation . . . ." *Id.* at 304. Here, while the government did not know who Vortman was at the time it started its sting operation, the government had sufficient reason to believe Playpen users – an identifiable group – were engaged in viewing and sharing child pornography. There is no doubt that Playpen was a site created for one sole purpose: to create a digital gathering place where individuals could view, distribute, and share child pornography while preventing detection. Accessing Playpen required several affirmative steps: (1) users had to download and install the Tor software on their computer; (2) users had to find Playpen's

[4] Vortman cited two cases where federal appellate courts found the government's conduct in distributing child pornography to not be outrageous conduct. *See United States v. Chin*, 934 F.2d 393, 399 (2d Cir. 1991) (no outrageous conduct where government sent defendant forty-eight previously seized images of child pornography); *United States v. Duncan*, 896 F.2d 271 (7th Cir. 1990) (no outrageous conduct where government sent defendant two magazine covers). Vortman argues his indictment warrants dismissal because, here, in contrast to *Chin* and *Duncan*, the Government's operation "resulted in an additional 9,000 images, 200 videos, and 13,000 links of child pornography being disseminated across the world . . . ." This argument is unavailing, however, because, unlike *Chin* and *Duncan*, the government did not actually distribute any child pornography. *See* ECF No. 54-4, at 5.

exact algorithmic site address to access it; (3) users had to input Playpen's address – random sequence of characters and all – into the Tor browser; (4) upon accessing Playpen's home site, users would need to ignore the two images of partially clothed prepubescent females with their legs spread apart – a likely preview of the illicit content on the website; and (5) to get beyond the homepage, users would need to register a new account, a process which explicitly advised users to provide a false email address in order to avoid detection. Given the affirmative steps needed to login to Playpen, the government had sufficient reason to believe Playpen's users were knowingly accessing the website to receive and distribute child pornography.

The third and fourth *Black* factors also weigh against dismissal. The third *Black* factor, "the government's role in creating the crime of conviction", looks at "whether the government approached the defendant initially or the defendant approached the government agent, and whether the government proposed the criminal enterprise or merely attached itself to one that was already established and ongoing." *Id.* at 305 (citation omitted). And the fourth factor, "the government's encouragement of the defendants to commit the offense conduct," looks at the "extent to which the government encouraged a defendant to participate in the charged conduct . . . ." *Id.* at 307. Here, as stated above, Vortman accessed Playpen by his own free will; his actions were entirely voluntary, without government prodding. Also, here, the government did not create Playpen. Nor did it add content to the website, or even engage with Playpen users. *See* ECF No. 54-4, at 5. The government merely attached itself to an illicit website that was already "established and ongoing," as illustrated by the fact that Playpen had already been operating for approximately six or seven months prior to government seizure. *See id.* at 3.

The fifth *Black* factor, "the nature of the government's participation in the offense conduct", looks at three subfactors: duration, nature of the involvement, and necessity. *Black*, 733 F.3d at 308–09. Regarding duration, the Ninth Circuit has explained that longer operations are of greater concern than intermittent or short-term ones. *Id.* at 308. In *Greene v. United States*, 454 F.2d, 783, 786 (9th Cir. 1971) the court found outrageous

government conduct where the government's participation with a criminal enterprise lasted between two and one-half to three and one-half years. In contrast, here, the government's attachment to Playpen lasted less than two weeks. With respect to the nature of the involvement, courts look at "whether the government acted as a partner in the criminal activity, or more as an observer of the defendant's criminal conduct." *Id.* at 308. Here, the government acted as a mere observer. Again, the government did not distribute any child pornography, nor engage with Playpen's users. *See* ECF No. 54-4, at 5. The necessity subfactor looks at "whether the defendants would have had the technical expertise or resources necessary to commit such a crime without the government's intervention." *Black*, 733 F.3d. at 309. Here, based on Vortman's use of Playpen before the NIT warrant was deployed, it is clear Vortman had the technical expertise and resources needed to access and use Playpen. This case is unlike *United States v. Twigg*, 588 F.2d 373, 380–81 (3d Cir. 1978) where the government provided laboratory expertise to a defendant who had no prior knowledge of how to manufacture methamphetamine. The Court finds this factor weighs against dismissal.

The last and sixth *Black* factor, "the nature of the crime being pursued and necessity for the actions taken in light of the nature of the criminal enterprise", looks at the "need for the investigative technique that was used in light of the challenges of investigating and prosecuting the type of crime being investigated." *Black*, 733 F.3d. at 309. For example, in *United States v. Wiley*, 794 F.2d 514, 515 (9th Cir. 1986), the court refused to find the government's creation of a prison smuggling scheme as outrageous "[g]iven the difficulties of penetrating contraband networks in prisons." The court must also consider "the tools available to law enforcement agencies to combat [the crime]." *Twigg*, 588 F.2d at 378 n. 6. At the same time, the "government does not have free license to forgo reasonable alternative investigative techniques of identifying and targeting potential suspects before approaching them." *Black*, 733 F.3d. at 309–310. Relevant to the matter before this court, Congress has recognized "the production, distribution and sale of child pornography is often a clandestine operation." S. Rep. No. 95–438, at 5 (1977). The

difficulties law enforcement agents face in stopping and preventing such conduct are exacerbated with the creation of technologies that can conceal a person's identity in the digital realm. Indeed, in seeking the NIT warrant the government testified "investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried." Macfarlane Aff. ¶ 31. In light of these difficulties, the Court finds the government's conduct in apprehending Playpen users was reasonable.

In conclusion, this Court finds the government's conduct did not rise to the level of outrageous conduct warranting dismissal of Vortman's indictment. Accordingly, Defendant's motion to dismiss his indictment is DENIED.

III. MOTION TO SUPPRESS NIT SEARCH WARRANT

Vortman also filed a motion to suppress all evidence from the NIT warrant. Vortman essentially makes two arguments in support of this second motion. First, Vortman argues the NIT warrant was an "unlawful general warrant that violated the Fourth Amendment's particularity requirement." ECF No. 55-1, at 22. Second, Vortman argues the NIT warrant was void because it violated Rule 41(b) of the Federal Rules of Criminal Procedure ("Rule 41(b)"). *Id.* at 11. The court addresses both arguments below.

A. Fourth Amendment Warrant Requirements

a. Legal Standard

The Fourth Amendment to the U.S. Constitution provides:

> The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend IV. "As a prerequisite to establishing the illegality of a search under the Fourth Amendment, a defendant must show that he had a reasonable expectation of privacy in the place searched." *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). A valid warrant requires three things: (1) the warrant must be issued by a neutral

magistrate; (2) the warrant must be backed by probable cause; and (3) the warrant must particularly describe the things to be seized, as well as the place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979).

b. Discussion

Vortman does not contest that the NIT warrant was issued by a neutral magistrate. However, he does contend the NIT warrant lacked probable cause, ECF No. 61, at 9–11, and that it failed to meet the particularity requirement. ECF No. 55-1, at 22–23; ECF No. 61, at 11. The Court disagrees and finds the NIT warrant complied with Fourth Amendment requirements.

i. Defendant had a Reasonable Expectation of Privacy in His Personal Computer

As an initial matter, Vortman argues he had a reasonable expectation of privacy in his personal computer. *See* ECF No. 55-1, at 19. A reasonable expectation of privacy exists if a person can "demonstrate a subjective expectation that his activities would be private, and he [can] show that his expectation was one that society is prepared to recognize as reasonable." *United States v. Bautista*, 362 F.3d 584, 589 (9th Cir. 2004). In *United States v. Heckencamp*, 482 F.3d 1142 (9th Cir. 2007), this circuit held there is "a legitimate, objectively reasonable expectation of privacy in [a] personal computer." *Id.* at 1146.[5] Moreover, this same court held that "the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer." *Id.* The reasonable expectation of privacy in a personal computer was reaffirmed in *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008).

On a related note, this circuit has also held there is no reasonable expectation of privacy in the IP addresses of websites visited because individuals "should know that this

[5] Other circuits have also recognized a reasonable expectation of privacy in a personal computer. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d. Cir. 2004); Trulock *v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001).

information is provided to and used by internet service providers for the specific purpose of directing the routing information." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007). In *Forrester*, the court found no Fourth Amendment search occurred when the government physically installed a pen-register-like device ("mirror port") at the defendant's internet service provider's facility that allowed the government to record the to/from addresses of the defendant's email messages, the IP addresses of the websites defendant visited, and the total volume of information sent to or from his account. *Id.* at 505. The *Forrester* court based this holding on *Smith v. Maryland*, 442 U.S. 735 (1979) where the Supreme Court held "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44.

Three district courts in this circuit that have addressed the NIT warrant have found *Forrester* stands for the proposition that there is no reasonable expectation of privacy in a person's IP address. *See United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4 (C.D. Cal. Aug. 8, 2016); *United States v. Michaud*, No. 3:15-cr-05352-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 1, 2016); *United States v. Henderson*, No. 15-cr-00565-WHO-1, 2016 WL 4549108, at *5 (N.D. Cal. Sept. 1, 2016). However, unlike the facts in *Forrester*, where the individual was openly conveying his IP address to third parties by using the open internet, here, Vortman was *not* using the open internet and his IP address was taken directly from his computer using the NIT. These differences are most certainly significant and distinguish the present case from *Forrester*. *See United States v. Hammond*, No. 16-cr-00102-JD-1, 2016 WL 7157762 (N.D. Cal. Dec. 8, 2016); *United States v. Croghan*, Nos. 1:15-cr-48 & 1:15-cr-51, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *United States v. Darby*, No. 2:16cr36, 2016 WL 3189703 (E.D. Va. Sept. 9, 2016); *United States v. Adams*, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016). In short, *Forrester* does not apply here.

The Court's reasoning is further buttressed by the Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473 (2014). In *Riley*, the government argued that the third party doctrine allowed law enforcement officers to always search the call log of a cell phone

found on an arrestee's person at the time of their arrest. *Id*. at 2492. However, despite the fact that the contents of a cell phone's call log would have likely been disclosed to a third party when the arrestee made the calls, the Court found that obtaining this information directly from the phone – as opposed to obtaining it from a third party – constituted a search. *Id.* at 2492-93. The Court also recognized several privacy concerns involved with allowing law enforcement officials to always search the cell phones of arrestees without a warrant: given the fact that today's cell phones have an immense storage capacity, they allow collection of many types of data dating back to the purchase of the phone (or further), which allow the reconstruction of a person's private life. *Id.* at 2489. These concerns apply equally, and perhaps with greater force, to a private computer. Thus, even assuming there is no reasonable expectation of privacy in one's IP address, the government must obtain a warrant if it seeks to extract the information directly from a person's personal computer. *See United States v. Anzalone*, No. 15-10347-PBS, 2016 WL 5339723, at *6 (D. Mass. Sept. 22, 2016).

ii. The NIT Warrant was Supported by Probable Cause

Probable cause requires only a "fair probability" that contraband or evidence is located in a particular place. *United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2007) (citing *Illinois v. Gates*, 462 U.S. 213, 246 (1983)). It does not require certainty or preponderance of the evidence. *Id.* Whether fair probability exists is a "commonsense, practical question" that looks at the totality of the circumstances, including reasonable inferences. *Id.* Moreover, a magistrate judge's determination on the existence of probable cause should be paid great deference. *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006).

Vortman argues the NIT warrant lacked probable cause because the NIT was deployed "whenever anyone *simply logged onto the site*," rather than being deployed when someone actually downloaded child pornography. ECF No. 61, at 13 (emphasis in original). As a result, Vortman argues, the NIT could have been deployed against individuals who "stumbled onto the site, looked around, decided that this wasn't what they

wanted, and left without downloading anything," or against individuals who were using Playpen to access the non-pornographic child erotica, non-nude pictures, artwork, or stories. *Id.* at 14.

On this issue, the *United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006) case is helpful to the Court's analysis. In that case the government had seized a child pornography website on the open internet and used the website's membership records to obtain a search warrant against the defendant, a subscriber of the seized website. The defendant sought to suppress over 100 images of child pornography and erotica seized from his computer. *Id.* at 1066. The defendant claimed the search warrant used to search his computer lacked probable cause because it contained no evidence the defendant "actually downloaded or possessed child pornography." *Id.* The defendant also argued there was no probable cause because the website also contained legal content such as adult pornography and child erotica. *Id.* at 1070. The Ninth Circuit disagreed and found the warrant was backed by probable cause because: (1) the defendant took affirmative steps to become a member of the site; (2) the website advertised pictures of adolescent girls; (3) the website offered images of adolescent females engaged in sexually explicit conduct; (4) the defendant remained a member for over two months, even though he could have cancelled at any time; (5) the defendant had access to hundreds of child pornography images; and (6) the defendant was likely to have seen images of nude prepubescent females with captions describing them as twelve to seventeen-year-old girls. *Id.* at 1068. Ultimately, the court rejected the defendant's argument "that a search warrant for child pornography may issue only if the government provides concrete evidence, without relying on any inferences, that a suspect *actually* receives or possesses images of child pornography." *Id.* at 1074 (emphasis in original).

The circumstances surrounding Playpen provide an equally strong case – if not stronger – for finding probable cause here than the facts did in *Gourde*. First, as discussed above, there is no question that individuals who accessed and logged into Playpen took several affirmative steps to do so. Because Playpen was a Tor hidden service with an

algorithm-generated site name, it would be extremely unlikely for somebody to "stumble" onto the site. And even assuming someone were to accidentally stumble onto Playpen's home site by entering the wrong website name or clicking on a non-descript link, the NIT would *not* be deployed at the instant a person merely visited the Playpen site; the NIT would only be deployed against individuals who logged into Playpen by entering both a username and password. ECF No. 83-1, at 3. Vortman downplays the effort needed to "simply log[] onto the site." ECF No. 61, at 13. Accessing Playpen, creating a user account, and logging into Playpen required several affirmative steps. This Court agrees that "anyone who ended up as a registered user on [Playpen] was aware that the site contained, among other things, pornographic images of children." *United States v. Epich*, No. 15-cr-163-PP, 2016 WL 953269, at *1 (E.D. Wis. Mar. 14, 2016). Second, the warrant was replete with evidence that Playpen was being used to host and distribute child pornography. There is no dispute that Playpen hosted thousands of images and hundreds of videos of children engaged in sexually explicit conduct, that users had access to this material when logged into the site, and that the titles of the site's forums and sub-forums clearly identified Playpen's primary content as child pornography. Vortman's assertion that the NIT warrant lacked probable cause because Playpen hosted legal content, such as erotic stories and non-nude images of children, is unavailing. The Ninth Circuit rejected nearly identical arguments in *Gourde* because there the evidence was "unequivocal" that the seized website's primary content consisted of child pornography. *See id.* at 1070. Here, like *Gourde*, the evidence is unequivocal that Playpen's primary content is child pornography.

In sum, the Court finds it did not defy logic, based on the totality of the circumstances, for the magistrate judge to determine there was a fair probability that individuals who accessed and logged into Playpen likely downloaded or distributed child pornography. Additionally, in further support of this Court's finding of probable cause, most, if not all, the courts that have analyzed whether the NIT warrant was supported by probable cause have found it was. *See Henderson*, 2016 WL 4549108, at *4 ("The courts

that have analyzed the NIT Warrant have all found that it was supported by probable cause.").

iii. The NIT Warrant Meets the Particularity Requirement

To satisfy the particularity requirement the warrant must "particularly describe both the place to be searched and the person or things to be seized," *United States v. Smith*, 424 F.3d 992, 1004 (9th Cir. 2005); *see also United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702 (9th Cir. 2009) ("Particularity means that 'the warrant must make clear to the executing officer exactly what it is that he or she is authorized to search for and seize.'"). At the same time, courts must consider the totality of circumstances, including the information available to the government, when determining the validity of a warrant. *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982). "Generic classifications in a warrant are acceptable only when a more precise description is not possible." *Id.* (citation omitted).

The Court agrees with the several other district courts, including the three district courts in this circuit, that have found the NIT warrant was sufficiently particular. *See United States v. Anzalone*, 2016 WL 5339723, at *7 ("Every court to consider this question has found the NIT search warrant sufficiently particular."). Indeed, the NIT warrant only permitted the government to collect a specific, limited set of data from "activating computers," which are defined as computers of any individual who logs into Playpen with a username and password. ECF No. 58-1, at 3. And because of the affirmative steps required to access Playpen, the warrant only applies to "a group that is necessarily actively attempting to access child pornography." *Henderson*, 2016 WL 4549108, at *4. Accordingly, the government was not required to only target administrators or users which "used the site regularly and aggressively," as Vortman suggests. ECF No. 55-1, at 27–28.

Vortman also argues the NIT warrant was not particular because it "did not name any specific person" or "identify any particular computer to be searched." *Id.* at 29. However, this is exactly why the government chose to deploy the NIT warrant: the government could not rely on traditional investigative methods to identify the identities of

Playpen users or their locations. *See* ECF No. 58-1, at 27. In other words, a more precise description of the persons or items to be searched was not plausible. Given the totality of the circumstances and the information available to the government, the NIT warrant was sufficiently particular to satisfy the Fourth Amendment.

B. Federal Rule of Criminal Procedure Rule 41(b)

a. Legal Standard

Rule 41(b) establishes the circumstances under which a magistrate judge may issue a warrant. As a general rule, a magistrate judge "has the authority to issue a warrant to search for and seize a person or property located *within* the district". Fed. R. Crim. P. 41(b)(1) (emphasis added). However, exceptions apply where a person or property might move or be moved outside the district before the warrant is executed, *id.* § (b)(2), when the government is investigating terrorism, *id.* § (b)(3), when a tracking device installed inside the district travels outside the district, *id.* § (b)(4), and where crimes occur in a U.S. territory, possession, commonwealth, or other U.S. lands that are not states, *Id.* § (b)(5).

Suppression of evidence obtained through a search that violated Rule 41(b) is required only if: (1) the violation arises to a constitutional magnitude; (2) the defendant was prejudiced; or (3) the government acted in intentional and deliberate disregard of the Rule. *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005).

b. Discussion

i. The NIT Warrant Violates Rule 41(b)

Vortman makes three arguments in support of his motion to suppress: (1) the NIT warrant failed to comply with Rule 41(b) because it authorized searches on "activating computers" outside the Eastern District of Virginia; (2) the Rule 41(b) violation was a constitutional violation which requires suppression of the evidence; and (3) if the Court decides the violation was not constitutional and therefore technical, Vortman was prejudiced.

The government responds contending the warrant complied with Rule 41(b) because the NIT warrant operated as a tracking device under Rule 41(b)(4). In essence,

the government argues the following: (1) the NIT constitutes a tracking device because its primary purpose is to determine the actual location of Playpen users; (2) the NIT was installed within the magistrate's district when it was installed on the server hosting the Playpen website; (3) when users logged onto Playpen they "digitally traveled" to the Eastern District of Virginia; and (4) the NIT would then track the users back to their home computers and disclose their identification information to the government. ECF No. 59, at 19–21. Although some courts have found the NIT warrant to be properly authorized under Rule 41(b)(4)[6], this Court agrees with the majority of courts to address this issue: the NIT was not a tracking device.

The term "tracking device" in Rule 41(b) means "an electronic or mechanical device which permits the *tracking of the movement* of a person or object." 18 U.S.C. § 3117 (2016) (emphasis added). Here, in contrast, "the NIT does not track; it searches." *United States v. Adams*, 2016 WL 4212079, at *6. Also, unlike a tracking device that primarily monitors movement, the NIT warrant relayed significantly more than just the location of the user's computer. *See Anzalone*, 2016 WL 53397223 at *9. And while the government argues Rule 41(b) should be "read flexibly so that it can keep up with technological innovations," ECF No. 59, at 19 (citing *United States v. New York Telephone Co.*, 434 U.S. 159, 169 (1977)), this court agrees that "[e]ven a flexible application of the Rule . . . is insufficient to allow the Court to read into it powers possessed by the magistrate that clearly are not contemplated and do not fit into any of the five subsections." *United States v. Werdene*, No. 15-434, 2016 WL 3002376, at *6 (E.D. Pa. May 18, 2016). Consequently, Rule 41(b) was violated because the NIT was not a tracking device and the NIT warrant authorized searches on computers outside the Eastern District of Virginia.

[6] *See, e.g.*, United States v. Darby, No. 2:16-cr-36, 2016 WL 3189703 (E.D. Va. June 3, 2016); United States v. Matish, No. 4:16-cr-16, 2016 WL 3545776, (E.D. Va. June 23, 2016); United States v. Eure, No. 2:16-cr-43, 2016 U.S. Dist. LEXIS 99168 (E.D. Va. July 28, 2016); United States v. Jean, No. 15-cr-50087-001, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); United States v. Lough, No. 1:16cr18, 2016 WL 6834003, at *6 (N.D. West Va. Nov. 18, 2016).

ii. Despite the Rule 41(b) Violation, Suppression of the NIT Warrant is Not Warranted

"Once a violation of Rule 41[] is identified, the next inquiry is whether the violation is 'fundamental' or 'non-fundamental.'" *United States v. Johns*, 948 F.2d 599, 603 (9th Cir. 1991). "A violation is 'fundamental' only where it, in effect, renders the search unconstitutional under traditional fourth amendment standards." *United States v. Vasser*, 648 F.2d 507, 510 (9th Cir. 1980). All other violations are "non-fundamental" or "technical" in which suppression is required only where there was prejudice or where there is evidence of deliberate disregard of Rule 41(b). *Id.*

Vortman argues the Rule 41(b) violation was fundamental because "[a] warrant issued by a judge who has no jurisdiction to issue it is no warrant at all." ECF No. 61, at 9 (citing *United States v. Levin*, No. 15-10271-WGY, 2016 WL 2596010, at *7 (D. Mass. May 5, 2016)). But this argument runs contrary to the Ninth Circuit's decision in *United States v. Ritter*, 752 F.2d 435 (9th Cir. 1985). In that case, the court was presented with an obvious violation of Rule 41(b) "when a search of [the defendant's] residence was conducted pursuant to a telephonic search warrant authorized by a state, rather than a federal, magistrate." *Id.* at 440. However, despite the state judge having no authority under Rule 41(b) to issue the warrant, the court upheld a finding that the error was merely technical and did not prejudice the defendant. *Id*. at 441.

Here, the government's violation of Rule 41(b) was technical. As explained above, the NIT warrant complied with the requirements of the Fourth Amendment – it was issued by a neutral magistrate, backed by probable cause, and sufficiently particular. *See Henderson*, 2016 WL 4549108, at *4 (finding a Rule 41(b) violation to be technical where the NIT Warrant complied with the Fourth Amendment); *Adams*, 2016 WL 4212079, at *7 (same).

The violation of Rule 41(b) also did not prejudice Vortman. Prejudice exists when "the search would not have occurred or would not have been so abrasive if law enforcement had followed the Rule." *Weiland*, 420 F.3d at 1071. Here, while the

magistrate judge violated Rule 41(b) by authorizing the deployment of the NIT on "activating computers" outside her jurisdiction, the government "*could* have installed copies of Playpen in every judicial district in the country . . . and then secured a corresponding number of Rule 41 warrants." *Acevedo-Lemus*, 2016 WL 4208436, at *7. Because the NIT warrant could have been deployed in a manner entirely consistent with Rule 41(b), the defendant was not prejudiced and suppression of the warrant is not appropriate.

iii. The Government Did Not Deliberately Disregard Rule 41(b).

Vortman also argues suppression is warranted because "almost every district court to consider this NIT warrant has found it to be unauthorized under Rule 41(b)," which illustrates the government's deliberate disregard of the rule. ECF No. 55-1, at 20. In support of this argument, Vortman cites *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), *United States v. Krueger*, 998 F. Supp. 2d 1032 (D. Kan. 2014), and *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). But these cases do little to bolster Vortman's contention. First, *Glover* and *Krueger* are both factually distinguishable. In *Glover*, the court was addressing a magistrate judge's authorization of a warrant to place a tracking device on a truck located outside the judge's district. *Glover*, 736 F.3d at 510. In *Krueger*, the district court was addressing whether a magistrate judge's authorization of a warrant allowing government agents to conduct a search outside of judge's district. *Kreuger*, 998 F. Supp. 2d at 1035. In both of these cases, the Rule 41 violation was obvious: the magistrate judges approved a search or seizure of physical property outside of their districts. Here, in contrast, the validity of the NIT warrant under Rule 41(b) was not at all obvious or clear-cut.

Second, several district courts have determined that the NIT warrant did not violate Rule 41(b). *See supra*, note 5. And even district courts that have rejected the NIT warrant as a tracking device have determined this theory is credible. *See, e.g.*, *Henderson*, 2016 WL 4549108, at *4 (recognizing the tracking device analogy is a "close question"); *Michaud*, 2016 WL 337263, at *6 (recognizing such arguments "are not unreasonable and

do not strain credulity"); *Acevedo-Lemus*, 2016 WL 4208436, at *7 ("It is not a stretch to say that the NIT functioned as a permissible 'tracking device'"). Based on these facts, it is apparent to the Court that the government could have reasonably believed the NIT warrant complied with Rule 41(b).

This leaves the Court to wrestle with *In re Warrant*. In that case, the court rejected the government's request for a search warrant that was similar to the NIT warrant in this case. The warrant sought authorization to "surreptitiously install data extraction software on the Target Computer," that once installed would have the capacity, among other things, to search the computer, identify the computer's location, and to transmit the extracted data to FBI agents. *Id.* at 755. Particularly relevant to this case, the court there found the requested warrant would likely violate Rule 41 because the location of the Target Computer was unknown, thus "permit[ting] FBI agents to roam the world" in search of evidence. *Id.* at 757. The court also rejected allowing the warrant device as a tracking device because "there was no showing that the installation of the 'tracking device' (i.e., the software) would take place within [the] district." *Id.* at 758. But even if this case had the potential of putting the government "on notice that courts disapproved of the government violating the jurisdictional limitations of Rule 41," ECF No. 55-1, at 21, this Court agrees that "[a] single court's decision analyzing a complicated and 'novel request' does not definitively demonstrate that the FBI deliberately disregarded [Rule 41]." *Henderson*, 2016 WL 4549108, at *5; *see also Michaud*, 2016 WL 337263, at *7 (same).

Lastly, Vortman argues the government knew the NIT warrant was impermissible because the government was aware that the Judicial Conference was accepting public comments on whether to amend Rule 41 to permit the exact search and seizure that occurred here. ECF No. 61, at 12. But an awareness that Rule 41 was subject to amendment merely demonstrates "recognized ambiguities in the Rule, not that [the government] acted with deliberate disregard for the rule." *Henderson*, 2016 WL 4549108, at *6. Vortman's argument was also rejected in *Michaud* because that court found "reasonable minds can differ as to the degree of Rule 41(b)'s flexibility in unchartered

territory." *Michaud*, 2016 WL 337263, at *7. A third district court in this circuit to analyze this argument found it supported the government's case because "[i]t would be strange indeed for the Court to suppress the evidence . . . in the face of a strong signal from the Supreme Court that Rule 41 should explicitly permit the issuance of warrants like the NIT Warrant." *Acevedo-Lemus*, 2016 WL 4208436, at *8. In sum, the Court finds the government did not deliberately disregard Rule 41(b).

iv. The Good Faith Exception Applies

Even assuming Vortman could establish a Fourth Amendment violation or show that he suffered prejudice, suppression is not warranted here because the government acted in good faith. The Supreme Court has held that the suppression of evidence is not warranted when officers rely on a warrant in good faith. *United States v. Leon*, 468 U.S. 897, 922 (1984). Good faith exists when the officer's conduct is objectively reasonable. *Id.* at 920. In cases when "an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope . . . . there is no police illegality and thus nothing to deter." *Id.* at 920–21.

The Court agrees with the three other district courts in this circuit that have concluded the good faith exception applied to the government's actions. *Acevedo-Lemus*, 2016 WL 4208436, at *8 ("FBI agents were, at every juncture, up front with the magistrate judge about how the NIT worked, what it would seize from 'activating computers,' and where 'activating computers' could be located. That Rule 41 may not yet be a perfect fit for our technological world does not mean that the FBI agents here acted in bad faith."); *Henderson*, 2016 WL 4549108, at *6 ("Here, the NIT was objectively reasonable – it was supported by substantial probable cause, was sufficiently particular in describing the people and places to be searched, and was issued by a neutral magistrate judge. The good faith exception applies and suppression is not appropriate."); *Michaud*, 2016 WL 337263, at *7 ("Because reliance on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good faith, and suppression is unwarranted."). Here, there is no evidence the government acted in bad faith or that the government acted in a manner

that was not objectively reasonable. Accordingly, evidence from the NIT warrant should not be suppressed.

IV. CONCLUSION

For the aforementioned reasons, Defendant's motion to dismiss his indictment and his motion to suppress the NIT warrant are DENIED.

IT IS SO ORDERED.

Dated: 12/16/16

THELTON E. HENDERSON
United States District Judge

United States District Court
Northern District of California